REMARKS

In response to the Office Action dated September 22, 2004, Applicant respectfully requests reconsideration and withdrawal of the rejections.

The Office Action states that a certified copy of French Priority Application No. 00/03919 has not been filed. However, the records of Applicant's undersigned representative show that a certified copy of the application was filed on June 14, 2001, together with the response to the Notice to File Missing Parts. The Examiner is respectfully requested to check the file to confirm whether the certified copy has been associated with the contents of the file.

Claims 1-3 and 5-8 were rejected under 35 U.S.C. § 101, on the grounds that they are directed to non-statutory subject matter. To remove the basis for this rejection, claims 1 and 5 have been amended to explicitly recite the step of generating at least two cryptographic keys from the integers a and b that have been confirmed to be co-prime with one another in accordance with the claimed steps. It is respectfully submitted that the generation of cryptographic keys according to the claimed process produces useful, concrete and tangible results, since such keys constitute the tools via which information is encrypted and decrypted in accordance with a public key cryptography protocol.

It is respectfully submitted that claims 6-8 defined statutory subject matter in their original form. In particular, these claims are directed to a portable electronic device having an arithmetic processor and program memory. The portable electronic device, e.g. a chip card, is a physical structure that is useful, concrete and tangible, and falls within the statutory category of a machine or article of manufacture. Reconsideration and withdrawal of the rejection under 35 U.S.C. § 101 is therefore respectfully requested.

Claims 4 and 5 were rejected under the first paragraph of 35 U.S.C. § 112, as failing to comply with the enablement requirement. The rejection states that the integers a and b are used for the creation of encryption and decryption keys, but do not constitute the keys themselves. In response thereto, claim 5 has been amended to recite that the cryptographic keys are generated "from" the integer pair a, b, to thereby preclude any erroneous interpretation that the integers themselves constitute the keys. In a similar manner, the amendment to claim 1 confirms that the cryptographic keys are generated from the integers a and b, and claim 4 has been amended to clarify that the so-generated keys form the encryption and decryption keys for a public key cryptograph protocol. Reconsideration and withdrawal of the rejection is respectfully requested.

Claims 1-6 were rejected under the second paragraph of 35 U.S.C. § 112, on the grounds that they were considered to be indefinite. It is respectfully submitted that the foregoing amendments to the claims remove any bases for this ground of rejection.

Claims 1-6 were rejected under 35 U.S.C. § 103 on the grounds that they were considered to be unpatentable over the article by Lidl and Pilz entitled "Applied Abstract Algebra", in view of the prior art described in the background portion of the application and the Schneier publication. It is respectfully submitted that these references do not suggest the claimed subject matter to a person of ordinary skill in the art whether they are considered individually or in combination.

The claimed invention is directed to public key cryptography, and more particularly to the generation of cryptographic keys for encrypting and decrypting information. The security of public key cryptography is based upon the generation of the keys from two numbers that are prime numbers, or at least prime with respect to one another. To successfully generate the keys, therefore, two selected numbers must be tested to ensure that they are co-prime with one another.

The claimed invention provides a particular method for conducting such a test. This method involves calculating a modular exponentiation that involves the Carmichael function, and testing whether the exponentiation is equal to 1.

The Lidl publication was apparently cited for its disclosure of the Carmichael function in connection with cryptographic keys. However, as acknowledged in the Office Action, the Lidl publication does not disclose a technique for verifying the co-primeness of two selected numbers that are used to generate the keys. To this end, therefore, the Office Action relies upon the disclosure in the background portion of the application, that it is known to verify co-primeness between two numbers that are selected to generate cryptographic keys. The rejection concludes that it would be obvious to employ this technique in the method disclosed in the Lidl publication.

It is respectfully submitted that, even if these teachings are combined in the manner suggested in the Office Action, the result would not lead one of ordinary skill in the art to the claimed invention. While the Lidl publication discloses that the Carmichael function is known, per se, it does not contain any suggestion that such a function should be used to verify the co-primeness of two numbers that are employed to generate cryptographic keys. Similarly, while the background portion of the application acknowledges that tests for co-primeness are known, it does not describe the use of the Carmichael function for such a purpose. There is nothing in the individual disclosures, nor in their combined teachings, which suggests the use of the Carmichael function in a modular exponentiation to verify the co-primeness of two numbers.

In setting forth the rejection, the Office Action appears to be suggesting that Lidl's use of the letter "n" is the same as Applicant's use of the letter "b". It is respectfully submitted, however, that these two reference characters do not represent the same entity. In the context of the present invention, the letter "b" represents one of the two integer values that are being tested for co-primeness. When they are determined to be co-prime, these values correspond to the factors "p" and "q" that are described in the Lidl publication. In contrast, the value "n" represents the *product* of "p" and "q". Thus, it can be appreciated that the modular exponentiation recited in the claims, namely, $a^{\lambda(b)}$ is not the same as the exponentiation , $a^{\lambda(n)}$ disclosed in the Lidl publication.

For at least the foregoing reasons, therefore, it is respectfully submitted that the Lidl publication does not suggest the claimed subject matter to a person of ordinary skill in the art, whether considered by itself or in combination with the prior art described in the background portion of the application. In addition to these distinctions, other differences are set forth in the claims. For example, claim 3 recites that the integer b is predetermined, and the value $\lambda(b)$ is calculated in advance and stored in memory. The rejection of this claim states that these features are implicit in the equation , $a^{\lambda(b)} = 1 \pmod{b}$. It is respectfully submitted, however, that this is not the case. When generating cryptographic keys, it is possible to dynamically generate both of the integers a and b each time a new set of keys is to be generated. In this case, the value for $\lambda^{(b)}$ must be calculated each time. In contrast to this approach, claim 3 is directed to an implementation of the invention in which the integer value is predetermined ahead of time, i.e., it is not dynamically generated for each new set of keys to be produced. As a result, the value of $\lambda^{(b)}$ can also be calculated ahead of time and stored in memory. This technique reduces the number of calculations that must be performed, and therefore the resources required, each time a new set of keys is generated. It is respectfully submitted that this claimed technique is not suggested by the equation identified in the rejection of the claim.

For similar reasons, it is respectfully submitted that the subject matter of claim 7 is not suggested by the references.

For the foregoing reasons, it is respectfully submitted that all pending claims are patentable over the prior art of record. Reconsideration and withdrawal of the rejections are therefore respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: December 22, 2004

By: ______________________
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620